STND-20080917C

STATEWIDE INFORMATION SECURITY STANDARD

Information Security Risk Assessment

Draft

Office of the Chief Information Officer

Department of Administration
Information Technology Services Division
PO Box 200113
Helena, MT 59620-0113
Tel: (406) 444-2700
FAX: (406) 444-2701

<Date Published>

Brian Schweitzer
Governor

State of Montana

DEPARTMENT OF ADMINISTRATION
Janet R. Kelly, Director

CHIEF INFORMATION OFFICER
Richard B. Clark

DRAFT STATEWIDE STANDARD: INFORMATION SECURITY RISK ASSESSMENT

EFFECTIVE DATE: JUNE 1, 2011
APPROVED: <DATE APPROVED>

I. Purpose

The purpose of this **Information Security Risk Assessment Standard** (Standard) is to establish the specifications and process requirements to implement the **Statewide Policy: Information Security Risk Assessment** (Policy) for computer and information systems security.

II. Authority

The State of Montana Chief Information Officer is responsible for developing policies, standards, and guidelines for addressing information security for agency operations and assets. This Standard is consistent with the requirements of the Montana Information Technology Act for securing information technology and §2-15-114, MCA. Security responsibilities of departments for data.

The Office of the Chief Information Officer of the State of Montana has developed this instrument to further the statutory responsibilities under §2-17-534, MCA. Security responsibilities of department, as delegated by the Director, Department of Administration.

III. Applicability

This Standard is applicable to parties subject to the **Statewide Policy: Information Security Risk Assessment**.

IV. Scope

This Standard specifies and requires the implementation of information security risk assessment controls for the information systems and assets managed or controlled by agencies.

This Standard encompasses information systems for which agencies have administrative responsibility, including systems managed or hosted by third-parties on agencies' behalf.

This Standard may conflict with other information systems policies currently in effect. Where conflicts exist, the more restrictive Standard governs. Future policies or standards will specifically identify and retire any superseded portions of current policies or standards.

V. Definitions

agency Any entity of the executive branch, including the university system. Reference §2-17-506(8), MCA.

Information Security The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. Reference 44 U.S.C., Sec. 3542.

Information System A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Reference 44 U.S.C. Sec. 3502.

Information Resources Information and related resources, such as personnel, equipment, funds, and information technology. Reference 44 U.S.C. Sec. 3502.

Information Technology Hardware, software, and associated services and infrastructure used to store or transmit information in any form, including voice, video, and electronic data. Reference §2-17-506(7), MCA.

Refer to the National Institute of Standards and Technology SP800-61 Revision 1 Computer Incident Handling Guide (NIST SP800-61), Appendix D - Glossary for a list of incident management-specific definitions.

Refer to the National Information Assurance (IA) Glossary, at http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf for common information systems security-related definitions.

Refer to the Statewide Information System Policies and Standards Glossary for a list of local definitions.

VI. Requirements

In compliance with the **Statewide Policy: Information Security Risk Assessment**, the requirements and specifications for this Standard are derived and adopted from the National Institute of Standards and Technology Special Publication 800-53 (NIST SP800-53) Recommended Security Controls for Federal Information Systems and Organizations (NIST SP800-53), Federal Information Processing Standard publications (FIPS PUB), and other NIST publications as specifically referenced herein.

A. Management Requirements

Each agency shall ensure that an organization structure is in place to:

1. Assign information security responsibilities.
2. Perform Risk Assessment for information systems.
3. Allocate adequate resources to implement Risk Assessment controls.

4. Establish and evaluate performance measures to assess implementation of this Standard and subordinate procedures.

5. Develop process(es) and procedure(s) to measure compliance with this Standard.

agency Heads: The agency head (or equivalent executive officer) has overall responsibility for providing adequate resources to support the management of information system security risk.

Information Security Officer: The Information Security Officer (also known as the Information Systems Security Officer) may be the same individual designated by the agency head to administer the agency's security program for data under §2-15-114, MCA. Security Responsibilities Of Departments For Data. Specific responsibilities under this Standard are:

1. Evaluate Risk Assessment issues within the agency and all component organizations.

2. Provide resolution recommendations to the agency head, attached agencies and division administrators, if any.

3. Develop agency policies, standards, and procedures as required.

4. Provides senior leadership input and oversight for all risk management and security activities across the agency (e.g., security categorizations, common security control identification) to help ensure consistent risk acceptance decisions.

5. Ensures that individual authorization decisions by authorizing officials consider all factors necessary for mission and business success agency-wide.

6. Provides an agency-wide forum to consider all sources of risk (including aggregated risk from individual information systems) to agency operations and assets, individuals, other organizations, and the State.

7. Ensures that security considerations are integrated into enterprise architectures, programming/planning/budgeting cycles, and acquisition/system development life cycles.

8. Promotes cooperation and collaboration among authorizing officials to include authorization actions requiring shared responsibility.

9. Identifies the overall risk posture based on the aggregated risk from each of the information systems and supporting infrastructures for which the agency is responsible.

10. Ensures that security activities (including the identification of deficiencies and gaps) are coordinated with appropriate agency entities (e.g., enterprise architects, information technology planners, planning/programming/budgeting officials).

11. Ensures that the shared responsibility for supporting agency mission/business functions using external providers of information and services (e.g., third-party providers) receives the needed visibility and is elevated to the appropriate decision-making authorities.

B. Performance Requirements

Each agency shall develop and implement Risk Assessment security controls based on an evaluation of information systems using the NIST ***risk management framework*** that:

1. Uses the categorization standards of:
   a. Federal Information Processing Standards Publication (FIPS PUB) 200 Minimum Security Requirements for Federal Information and Information Systems
   b. Federal Information Processing Standards Publication (FIPS PUB) 199 Standards for Security Categorization of Federal Information and Information Systems
2. Specifies levels of risk management standards and controls based upon the following requirements:
   a. As determined by completion of the ***risk management process*** described within NIST SP800-39 Managing Risk from Information Systems – An Organizational Perspective. After review of the risk assessment(s), agency management shall determine any changes in the level of process, standards and controls.

   Or,

   b. Implement the **lowest** level of Risk Assessment standards and controls based upon NIST SP800-53 Recommended Security Controls for Federal Information Systems, Annex 1, Low-Impact Baseline Risk Assessment (RA) family (known as **Annex 1**) not later than **September 1, 2010**.
3. Includes specific controls based on NIST SP800-39 Managing Risk from Information Systems and NIST SP800-30 Risk Management Guide for Information Technology Systems.
   a. Risk Management Framework. Reference: NIST SP800-39, paragraph 3.1:

      The agency uses a structured, flexible process and framework for managing risk related to the operation and use of information systems. The framework is used by the agency to determine the appropriate risk mitigation needed to protect ithe information systems and infrastructure supporting the agency's mission and business processes.

   b. Categorization of Information and Information Systems. Reference: NIST SP800-39, paragraph 3.2:

      The agency conducts a thorough analysis of the agency's mission and business processes informed by the agency's enterprise architecture, identifying the types of information that will be processed, stored, and transmitted by the information systems supporting those processes.

   c. Selection of Security Controls. Reference: NIST SP800-39, paragraph 3.3:

The agency selects appropriate security controls that can be specified for each information system to implement the agency's protection strategy.

d. Implementation of Security Controls. Reference: NIST SP800-39, paragraph 3.4

Security controls that are documented in approved security plans are allocated to specific information systems (i.e., system-specific controls and the system-specific portions of hybrid[1] controls areallocated to particular system components) and to the supporting infrastructure (i.e., common controls[2] and the non system-specific portions of hybrid controls are allocated to the information system environments of operation including facilities).

e. Assessment of Security Controls. Reference: NIST SP800-39, paragraph 3.5:

The agency assesses the implemented controls for effectiveness using the assessment procedures in NIST Special Publication 800-53A Guide for Assessing the Secuiry Controls in Federal Information Systems.

f. Authorizing Organizational Information Systems. Reference: NIST SP800-39, paragraph 3.6:

The agency authorizes the information systems following the guidance in NIST SP800-37, Revision 1 Guide for Security Authorization of Federal Information Systems. Authorization decisions are based on a determination, understanding, and explicit acceptance of risk to organizational operations and assets, individuals, other organizations, and the State arising from the operation and use of information systems. Authorizing officials weigh the near-term operational capability being gained by the mission/business process dependence on information and information systems with the potential loss of operational capability due to the susceptibility to the threats that result from this dependence.

g. Monitoring the Security State of the Organization. Reference: NIST SP800-39, paragraph 3.7:

The agency conducts comprehensive continuous monitoring programs to maintain on-going, up-to-date knowledge by senior leaders of the agency's security state and risk posture, and to initiate appropriate responses as needed when changes occur. Continuous monitoring programs include:

[1] Refer to NIST SP800-53 Recommended Security Controls for Federal Information Systems, Chapter Two for a description of "hybrid" controls.

[2] Refer to NIST SP800-53 Recommended Security Controls for Federal Information Systems, Chapter Two for a description of "common" controls.

- Determining if the security controls in organizational information systems and supporting infrastructure continue to be effective over time in light of the inevitable changes that occur in the systems as well as the environment in which the systems operate; and
- Causing the necessary steps of the risk management framework to be engaged to adequately address changes to include, re-categorizing information and information systems and responding to any changes in the FIPS 199 impact levels of the systems by appropriately adjusting security controls, and reauthorizing the systems, when required.

4. Implements this Standard through procedure(s).
5. Allocates adequate resources to perform risk assessments.
6. Reviews risk assessments, process and procedure(s) annually, and implement authorized changes to policy, standard(s), or procedure(s).
7. Is based upon the latest publicly available versions of publications referenced within this Standard *at the date of approval* of this Standard. (Note: Because newer versions of the publications referenced herein become available from time-to-time, each agency is encouraged to stay current by using the most recent versions, as deemed feasible by each agency. Future revisions of this Standard shall reference then currently-available versions.)

VII. Compliance

Compliance with this Standard shall be evidenced by adherence to the requirements specified above, as described in the referenced publications.

VIII. Change Control and Exceptions

Standard changes or exceptions are governed by the Procedure for Establishing and Implementing Statewide Information Technology Policies and Standards. Requests for a review or change to this instrument are made by submitting an Action Request form (at http://itsd.mt.gov/content/policy/policies/Administration/action_request.doc). Requests for exceptions are made by submitting an Exception Request form (at http://itsd.mt.gov/content/policy/policies/Administration/exception_request.doc). Changes to policies and standards will be prioritized and acted upon based on impact and need.

IX. Closing

For questions or comments about this instrument, contact the State of Montana Chief Information Officer at ITSD Service Desk (at http://servicedesk.mt.gov/ess.do), or:

PO Box 200113
Helena, MT 59620-0113
(406) 444-2700
FAX: (406) 444-2701

X. References

A. Legislation

- §2-15-114, MCA – Security Responsibilities of Departments for Data.
- §2-17-534, MCA - Security Responsibilities of Department.

B. Policies, Directives, Regulations, Rules, Procedures, Memoranda

- MOM 3-0130 Discipline
- Statewide Policy: Establishing and Implementing Statewide Information Technology Policies and Standards
- Statewide Procedure: Establishing and Implementing Statewide Information Technology Policies and Standards

C. Standards, Guidelines

- Guide To NIST Information Security Documents
- NIST SP800-39 Managing Risk from Information Systems
- NIST SP800-30 Risk Management Guide for Information Technology Systems
- NIST SP800-53 Recommended Security Controls for Federal Information Systems
- NIST SP800-53 Recommended Security Controls for Federal Information Systems, Annex 1, Low-Impact Baseline Risk Assessment (RA) family
- NIST SP800-53 Recommended Security Controls for Federal Information Systems, Annex 2, Moderate-Impact Baseline Risk Assessment (RA) family
- NIST SP800-53 Recommended Security Controls for Federal Information Systems, Annex 3, High-Impact Baseline Risk Assessment (RA) family
- Federal Information Processing Standards Publication (FIPS PUB) 200 Minimum Security Requirements for Federal Information and Information Systems
- Federal Information Processing Standards Publication (FIPS PUB) 199 Standards for Security Categorization of Federal Information and Information Systems

XI. Administrative Use

Product ID:	STND-20080917c
Proponent:	Chief Information Officer
Publisher	Office of the Chief Information Officer
Published Date:	<Date Published>
Version:	0.8.2
Version Date:	4/16/2009
Custodian:	Policy Manager
Approved Date:	<Date Approved>
Effective Date:	June 1, 2011
RIM Class:	Record
Disposition Instructions:	Retain for Record
Change & Review Contact:	ITSD Service Desk (at http://servicedesk.mt.gov/ess.do)
Review:	Event Review: Any event affecting this instrument may initiate a review. Such events may include a change in statute, key staff changes or a request for review or change.
Scheduled Review Date:	June 1, 2016
Last Review/Revision:	<None>
Changes:	